AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

receiving data from a network application program interface (API) of a sending client, the data comprising a portion of an event to be sent from the sending client to a receiving client;

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data;

creating a selector based on the selector data and using said selector to search a local sending client database of security associations for at least one selector/security association pair identifying a security association corresponding to the selector, said database storing a plurality of selector/security association pairs received from a key server corresponding to different timewise intervals of said event, the receiving client storing a receiving client database comprising a similar plurality of selector/security association pairs received from said key server;

applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data; and

sending the data to which the security operation has been applied to a network protocol layer of the sending client.

2. (Canceled)

3. (Currently Amended) The method of claim [[2]] 1 wherein the selector data is based at least in part on one of an internet protocol address taken from the data and a port indicator taken from the data.

4. (Previously Presented) The method of claim 1 wherein applying the security operation comprises at least one of:

attaching a header to the data, said header including a security operation tag; and

encrypting the data.

5. (Canceled)

6. (Currently Amended) A method comprising:

receiving data from a network protocol layer of a receiving client, the data comprising a portion of an event being received at the receiving client;

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data;

creating a selector based on the selector data and using said selector to search a receiving client database of security associations for at least one selector/security association pair identifying a security association corresponding to the selector, said receiving client database storing a plurality of selector/security association pairs received from a key server corresponding to different timewise intervals of said event;

applying the security operation to the data if the data is eligible wherein applying the security operation comprises using the security association on the at least a portion of the data; and

sending the data to which the security operation has been applied to a network application program interface (API) of the receiving client.

7. (Original) The method of claim 6 wherein determining if the data is eligible for a security operation comprises at least one of:

detecting a security operation tag in a header of the data; and

detecting failure of an integrity check on the data.

8. (Previously Presented) The method of claim 6, said event being sent from a sending client to the receiving client, the sending client storing a sending client database comprising a similar plurality of selector/security association pairs respectively corresponding to said different timewise intervals of said event.

9. (Currently Amended) The method of claim 8, said ~~receiving client database selector/security association pairs and said~~ sending client database selector/security association pairs having been received from [[a]] said key server.

10. (Previously Presented) The method of claim 6 wherein determining if the data is eligible for the security operation comprises determining that the data is not eligible for the security operation if the selector cannot be created based on the selector data, and

wherein said data is sent to the network API of the receiving client without an applied security operation if it is so determined that the data is not eligible.

11. (Canceled)

12. (Canceled)

13. (Previously Presented) The method of claim 6 wherein the security association comprises at least one of:

applying encryption to the data;

removing special packaging from the data;

applying decryption to the data; and

performing an integrity check on the data.

14. (Currently Amended) A machine readable storage medium having stored thereon machine executable instructions, execution of said machine executable instructions being operable to implement a method comprising:

receiving data from a network application program interface (API) of a sending client, the data comprising a portion of an event to be sent from the sending client <u>to a receiving client</u>;

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data;

creating a selector based on the selector data and using said selector to search a local sending client database of security associations for at least one selector/security association pair identifying a security association corresponding to the selector, said sending client database storing a plurality of selector/security association pairs received from a key server corresponding to a succession of timewise intervals of said event, the receiving client storing a receiving client database comprising a similar plurality of selector/security association pairs received from the key server;

applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data; and

sending data to which the security operation has been applied to a network protocol layer of the sending client.

15. (Canceled)

16. (Previously Presented) The machine readable storage medium of claim 14 wherein the selector data is based at least in part on one of an internet protocol address taken from the data and a port indicator taken from the data.

17. (Previously Presented) The machine readable storage medium of claim 14 wherein applying the security operation comprises at least one of:

attaching a header to the data, said header including a security operation tag;

performing an integrity check; and

encrypting the data.

18. (Canceled)

19. (Currently Amended) A machine readable storage medium having stored thereon machine executable instructions, execution of said machine executable instructions being operable to implement a method comprising:

receiving data from a network protocol layer of a receiving client, the data comprising a portion of an event being received at the receiving client;

determining if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data;

creating a selector based on the selector data and using said selector to search a local receiving client database of security associations for at least one selector/security association pair identifying a security association corresponding to the selector, said receiving client database storing a plurality of selector/security association pairs received from a key server corresponding to a succession of timewise intervals of said event;

applying the security operation to the data if the data is eligible, wherein applying the security operation comprises using a security association on the at least a portion of the data; and

sending the data to which the security operation has been applied to a network application program interface (API) of the receiving client.

20. (Previously Presented) The machine readable storage medium of claim 19 wherein determining if the data is eligible for a security operation comprises at least one of:

detecting a security operation tag in a header of the data; and

detecting failure of an integrity check on the data.

21. (Previously Presented) The machine readable storage medium of claim 19, said event being sent from a sending client to the receiving client, the sending client storing a sending client database comprising a similar plurality of selector/security association pairs respectively corresponding to said succession of timewise intervals of said event.

22. (Currently Amended) The machine readable storage medium of claim 21, said ~~receiving client database selector/security association pairs and said~~ sending client database selector/security association pairs having been received from [[a]] said key server.

23. (Previously Presented) The machine readable storage medium of claim 19 wherein determining if the data is eligible for the security operation comprises determining that the data is not eligible for the security operation if a selector cannot be created based on the data, and wherein said data is sent to the network API of the receiving client without an applied security operation if it is so determined that the data is not eligible.

24. (Canceled)

25. (Canceled)

26. (Previously Presented) The machine readable storage medium of claim 19 wherein the security association comprises at least one of:

applying encryption to the data;

removing special packaging from the data;

applying decryption to the data; and

performing an integrity check on the data.

27. (Currently Amended) A management server apparatus at a sending client in which an event having an event duration is transmitted from the sending client to a receiving client, ~~the event having a duration and being divided into a succession of timewise intervals that are relatively short compared to said event duration~~, comprising:

a processing unit to:

receive a plurality of selector/security association pairs from a key server corresponding to [[said]] a succession of timewise intervals of said event that are relatively short compared to said event duration;

receive data from a network application program interface (API) of the sending client, the data including a portion of the event within one of said timewise intervals,

determine if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data, create a selector based on the selector data, wherein said selector indicates at least a portion of the data and a security association associated with at least one of said selector/security association pairs received from the key server,

apply the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data, and

send the data to which the security operation has been applied to a network protocol layer of the sending client.

28. (Currently Amended) A management server apparatus at a receiving client receiving an event transmitted from a sending client, the event having [[a]] an event duration ~~and being divided into a succession of timewise intervals that are relatively short compared to said event duration~~, comprising:

a processing unit to:

receive a plurality of selector/security association pairs from a key server corresponding to [[said]] a succession of timewise intervals of said event that are relatively short compared to said event duration;

receive data from a network protocol layer of the receiving client, the data including a portion of the event within one of said timewise intervals,

determine if the data is eligible for a security operation, wherein eligibility is determined by selector data contained in the data, create a selector based on the selector data, said selector indicating at least a portion of the data and a security association associated with at least one of said selector/security association pairs received from the key server;

apply the security operation to the data if the data is eligible, wherein applying the security operation comprises using the security association on the at least a portion of the data, and

send the data to which the security operation has been applied to a network application program interface (API) of the receiving client.